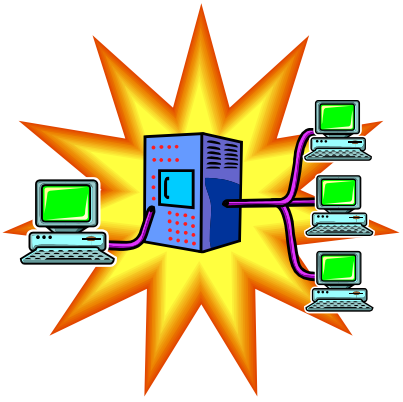
SPAWAR Systems Center Charleston

# DoD PKI

## Server Certificate Enabling For

## Microsoft Internet Information Server 5.0

### Step 1: Generating a Key Pair and Requesting a Certificate



# PK-Enabling For Microsoft Internet Information Server (IIS 5.0)

## Step 1: Generating a Key Pair and Requesting a Certificate

This Document details how to generate a PKI key pair and request a server certificate using Microsoft Internet Information Server 5.0. It covers step 1 of a 2-step process. "Server Certificate Enabling for Microsoft Internet Information Server 5.0: Step 2: Obtaining/Installing a PKI Certificate" is a follow-up document. It details how to obtain and install a PKI server certificate as well as how to make the web server secure (https).

## Step 1: Generating a Key Pair and Requesting a Certificate

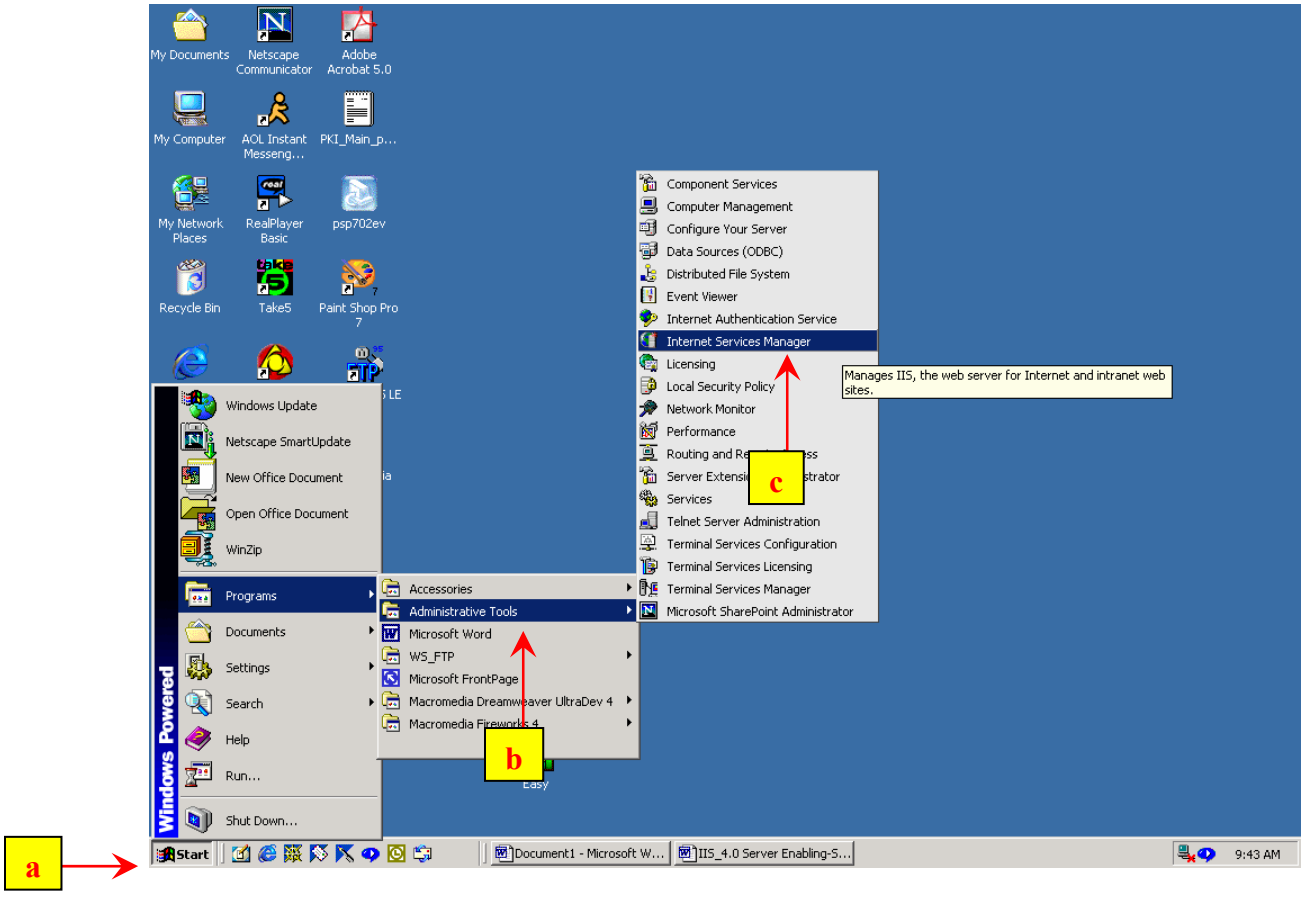
# PK-Enabling For Microsoft Internet Information Server (IIS 5.0)

**The following must be installed before attempting to install DoD certificates onto your server. **ALL SOFTWARE LISTED BELOW MUST BE 128-BIT.**

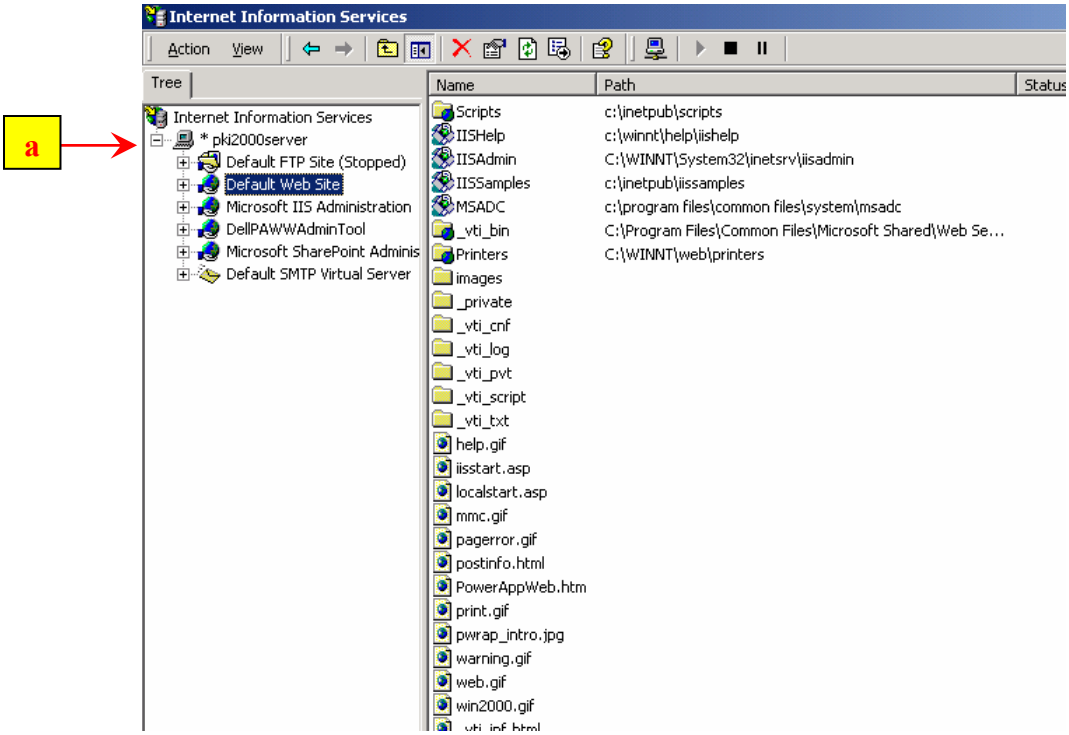
1. Windows 2000 Server
2. Netscape 4.5 or greater
3. IE 5.0 or greater

## Generating a Key Pair

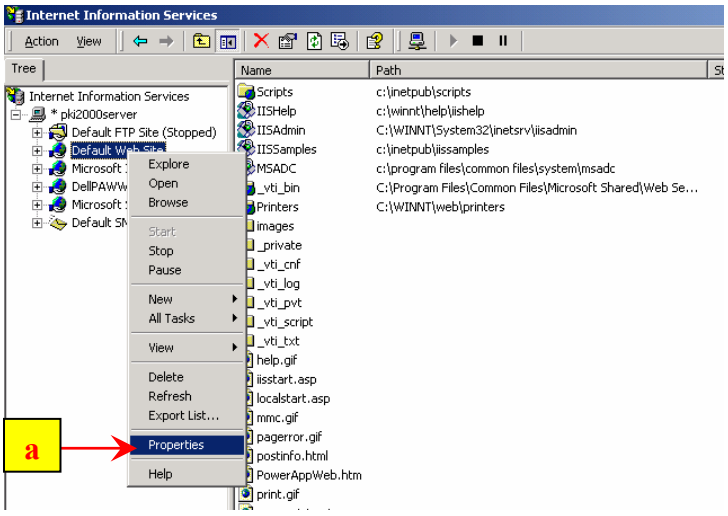
1) Generating a Key File.
   a) Click **Start, Programs.**
   b) **Administrative Tools.**
   c) **Internet Service Manager.**



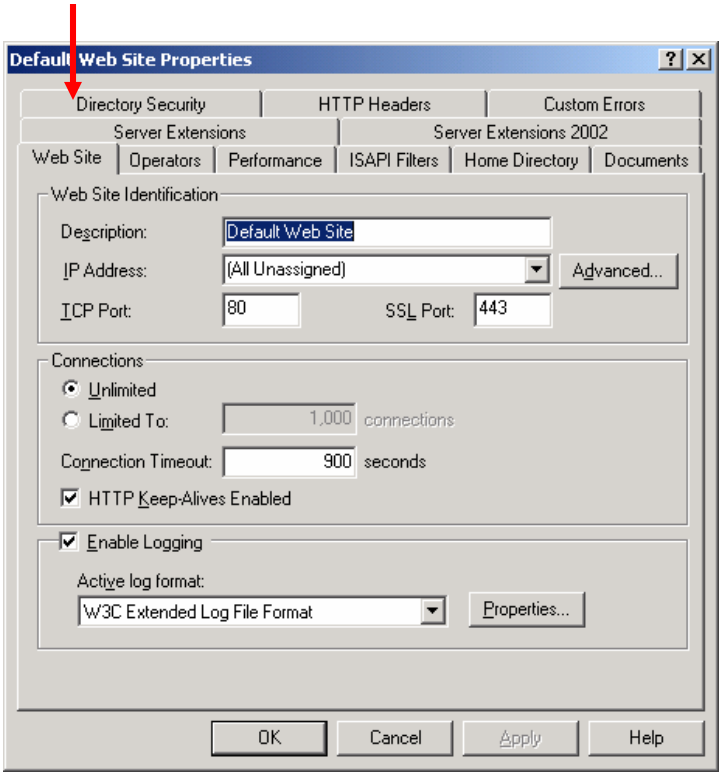
2) Expand the Server
   a) Click on * ***your server name***.



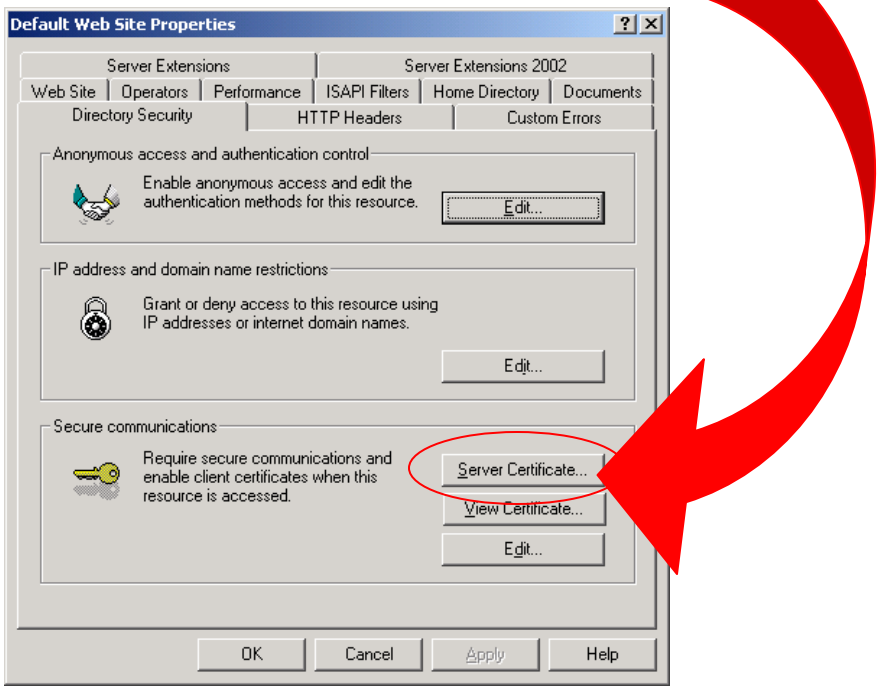

3) Open the Properties Dialog Box.
   a) Right click on the desired web site and choose **Properties**. The Administrative Web Site Properties dialog box appears.



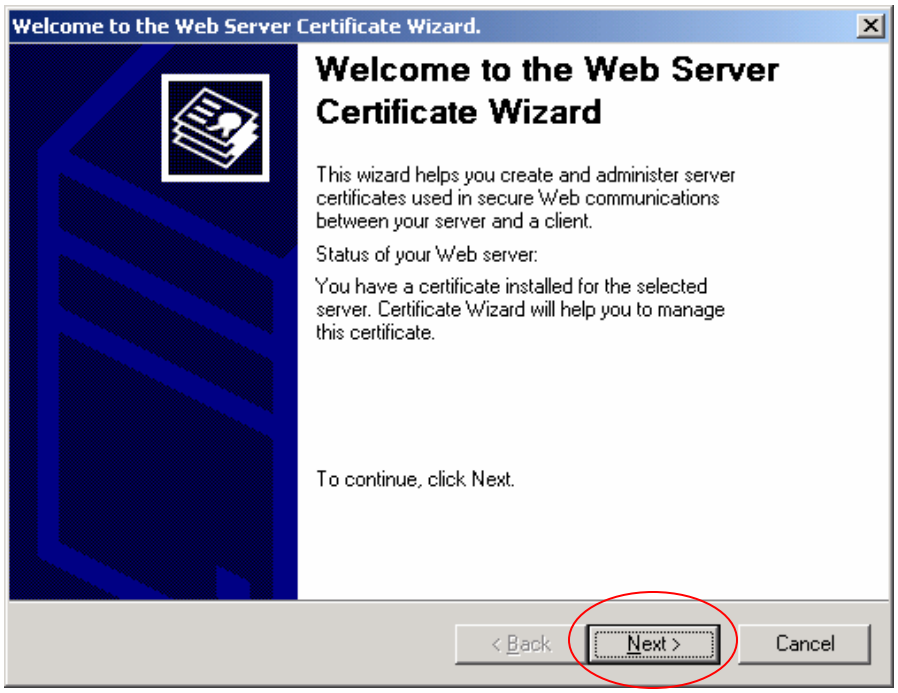
4) Click on the **Directory Security Tab**.



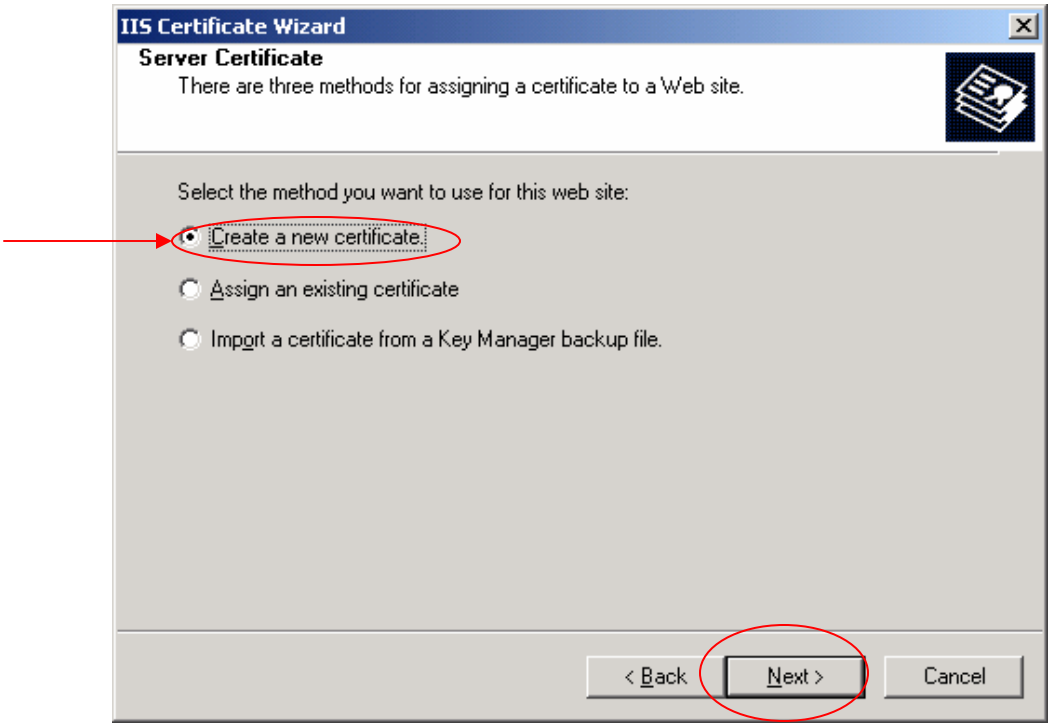

5) Under Secure Communications, click **Server Certificate**



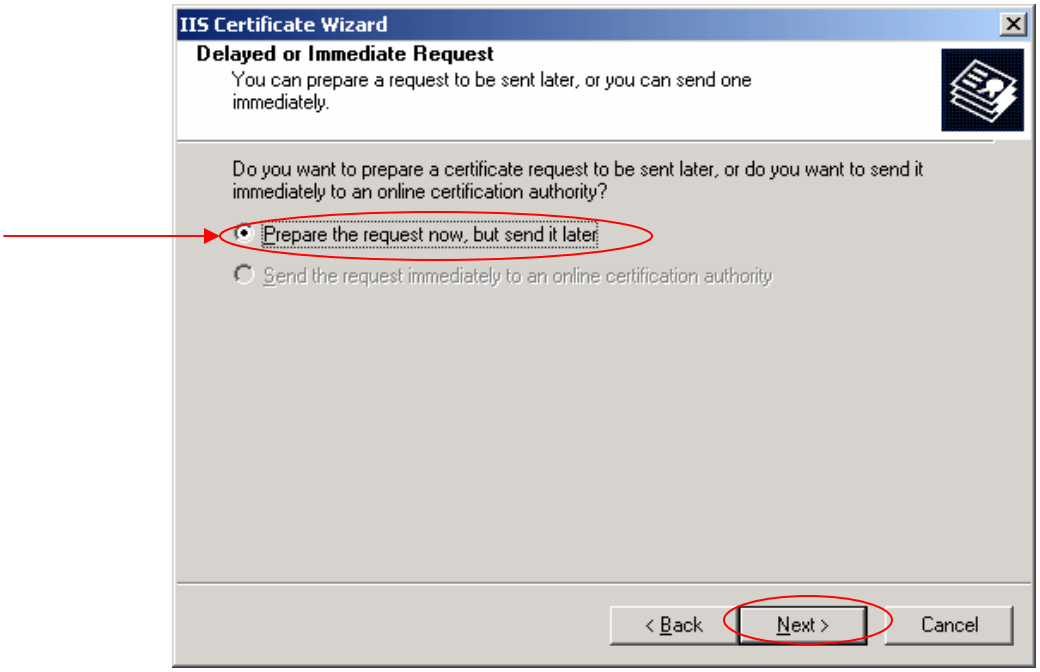
6) Click **Next**.



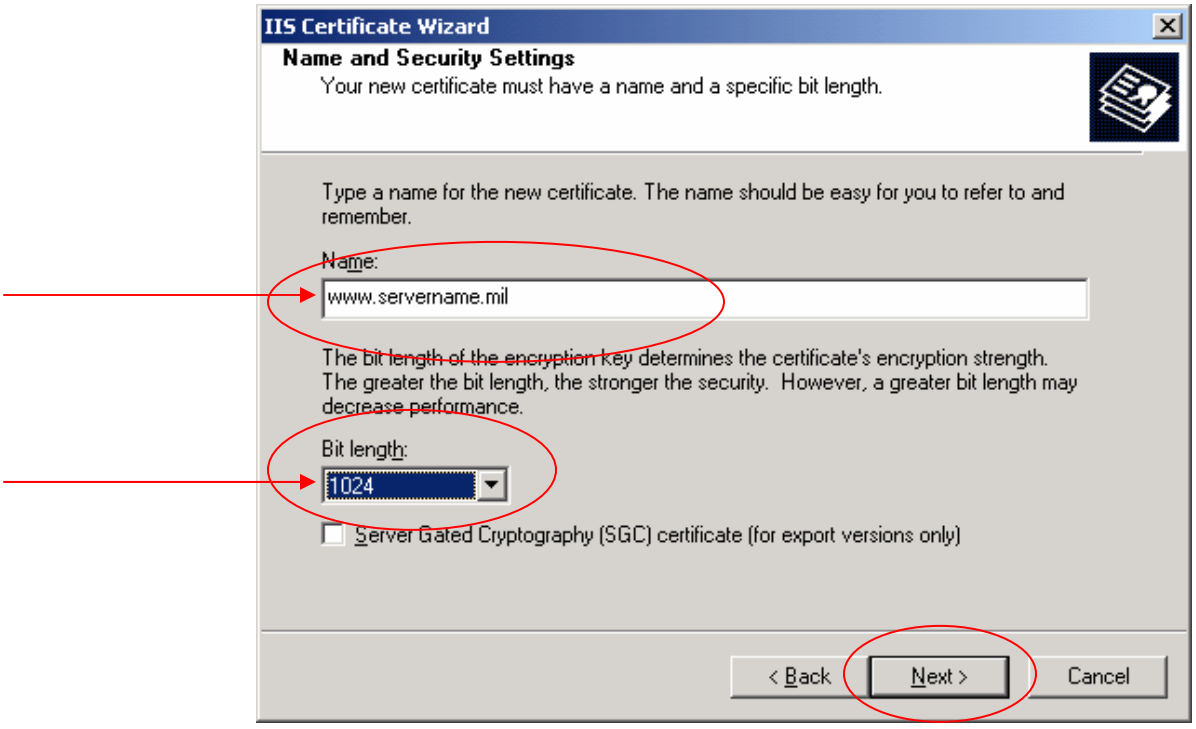

7) Confirm that the **Create a New Certificate** button is selected and then click **Next**.



8) Click the **Prepare the request now, but sent it later** button and then click **Next**.

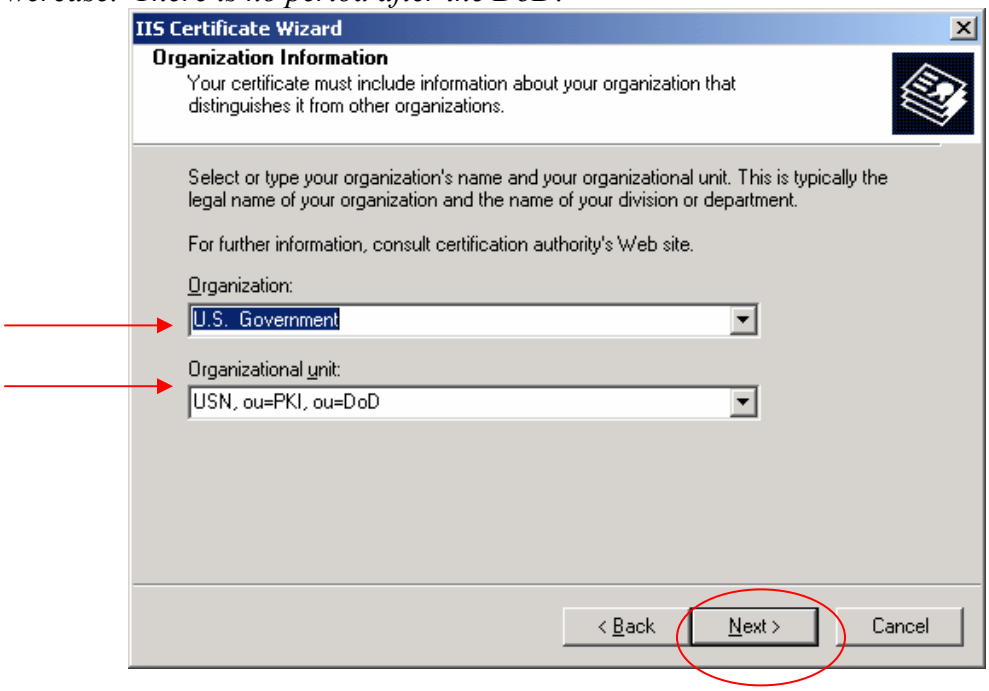



9) Fill in the **Name field with the exact url** you type to access your website. In the **Bit Length** field change your selection to **1024**. Click **Next**.

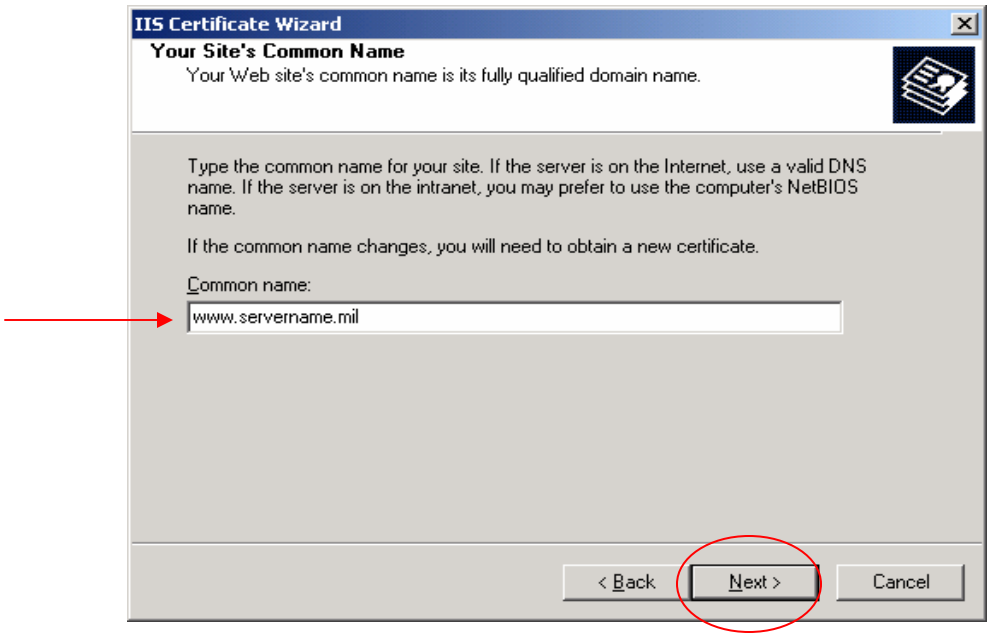


10) In the Organizational field, type **U.S. Government**, and in the Organizational Unit box, type **USN OU=PKI OU=DoD**. Click **Next**.

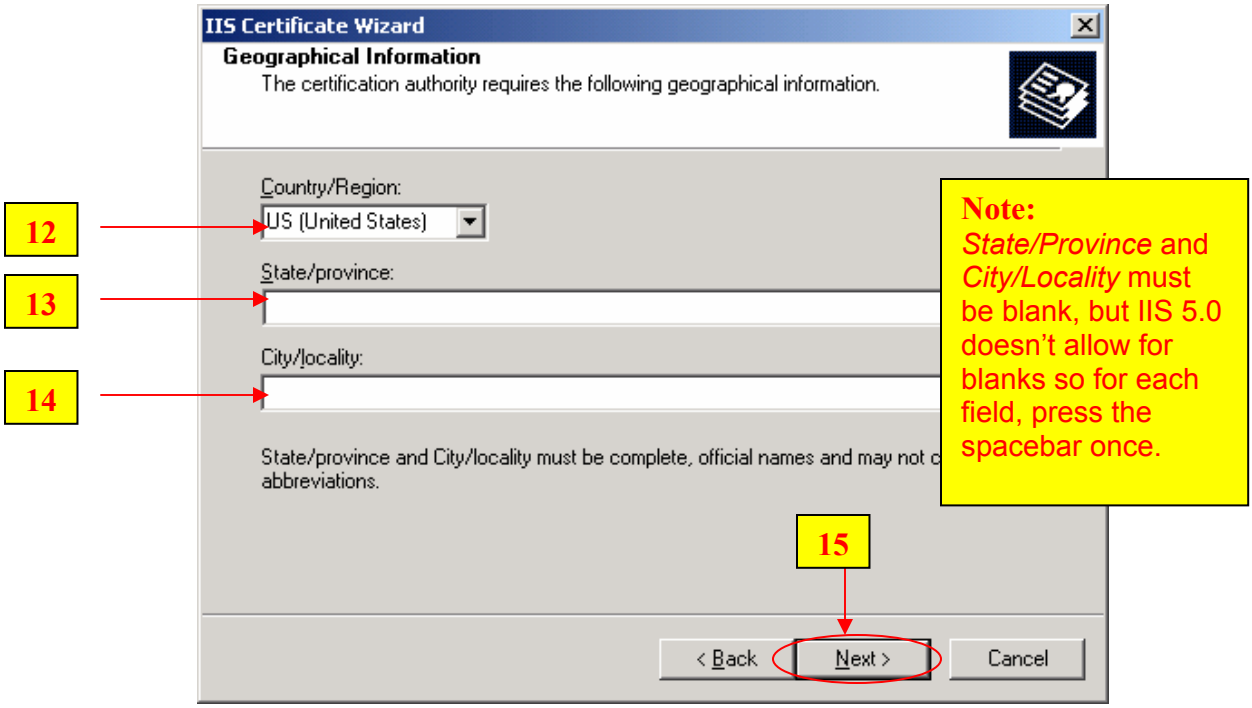
***NOTE:** *The text is case-sensitive. There is a space after the letters **U.S.** and the word **Government**. There is also a space after **USN** and the letters **OU=PKI**. There is another space after the letters **PKI** and the letters **OU=DoD**. The letter "**o**" in **DoD** is lowercase. There is no period after the **DoD**.*



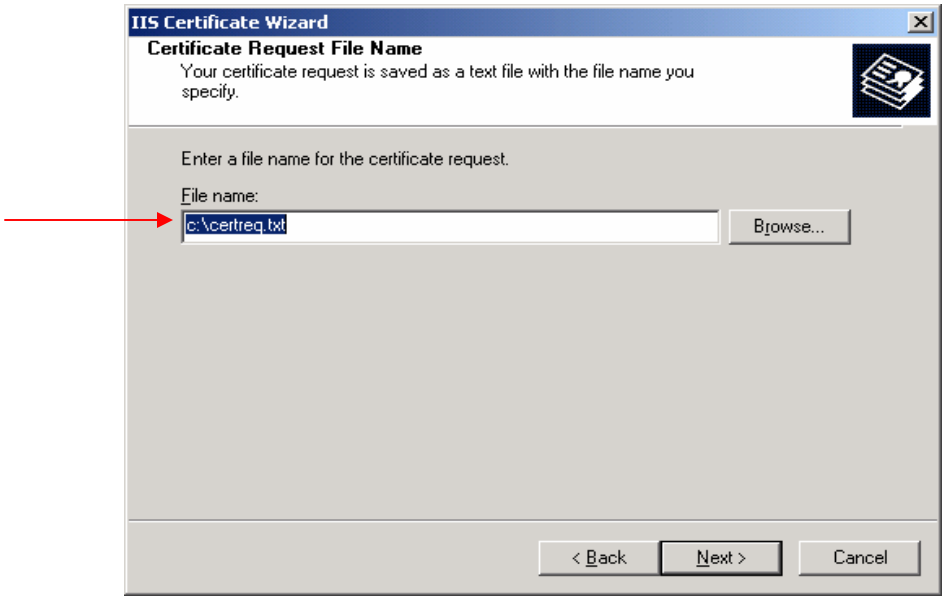

11) In the **Common Name** text box, type the domain name of your web site, for example, *www.basename.navy.mil* and then click **Next**. The **Common Name** is the fully qualified domain name (FQDN) of the server that the certificate will be installed on.



12) In the **Country/Region** box, type **US** (United States). Normally, this should be the default.
13) In the **State/province** box, press **Spacebar**. To move to the **City/locality** field, press **TAB** or click the **City/locality** box.
14) In the **City/locality** box, press **Spacebar**.
15) Click **Next**.

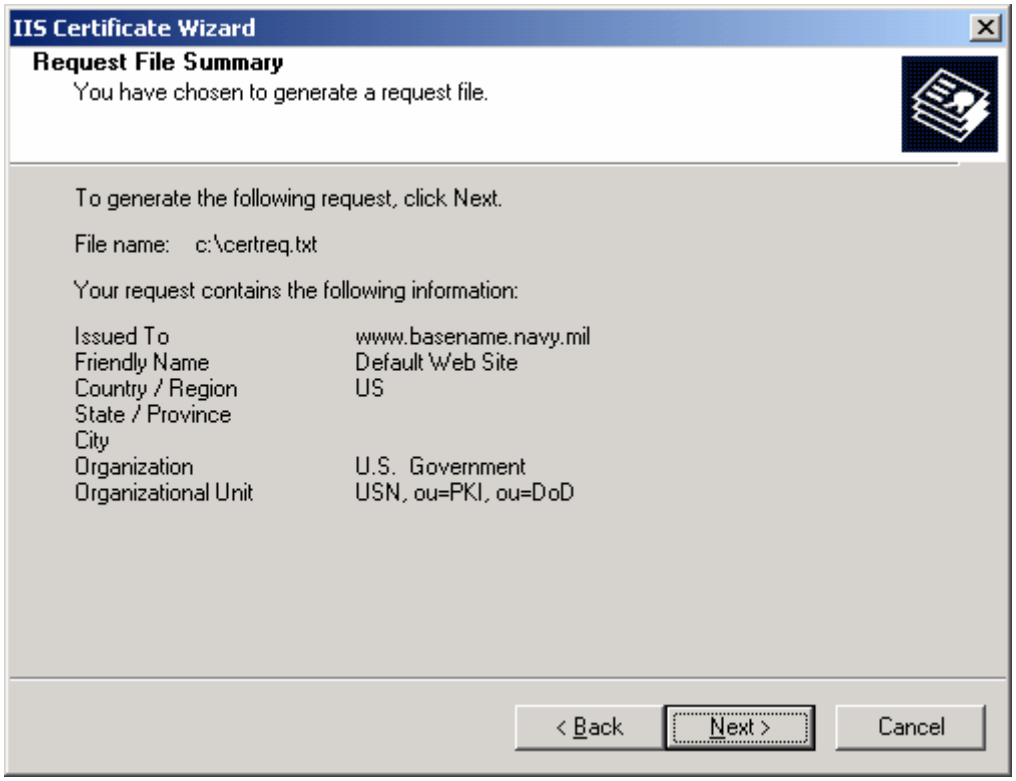



16) In the **File name** box, enter a file name. Remember the folder where the file is save. You may also click **Browse** to locate the desired folder. The file name should have a **.txt** extension and is saved in a text format. Click **Next**.



17) The **Request File Summary** screen appears. Read through the summary information on the screen.

- If changes need to be made, click **Back** as many screens as necessary to make changes.
- After making the changes, click **Next** as many times as needed to get back to this screen.
- Click **Next** to display the **Completing the Web Certificate Wizard** screen.



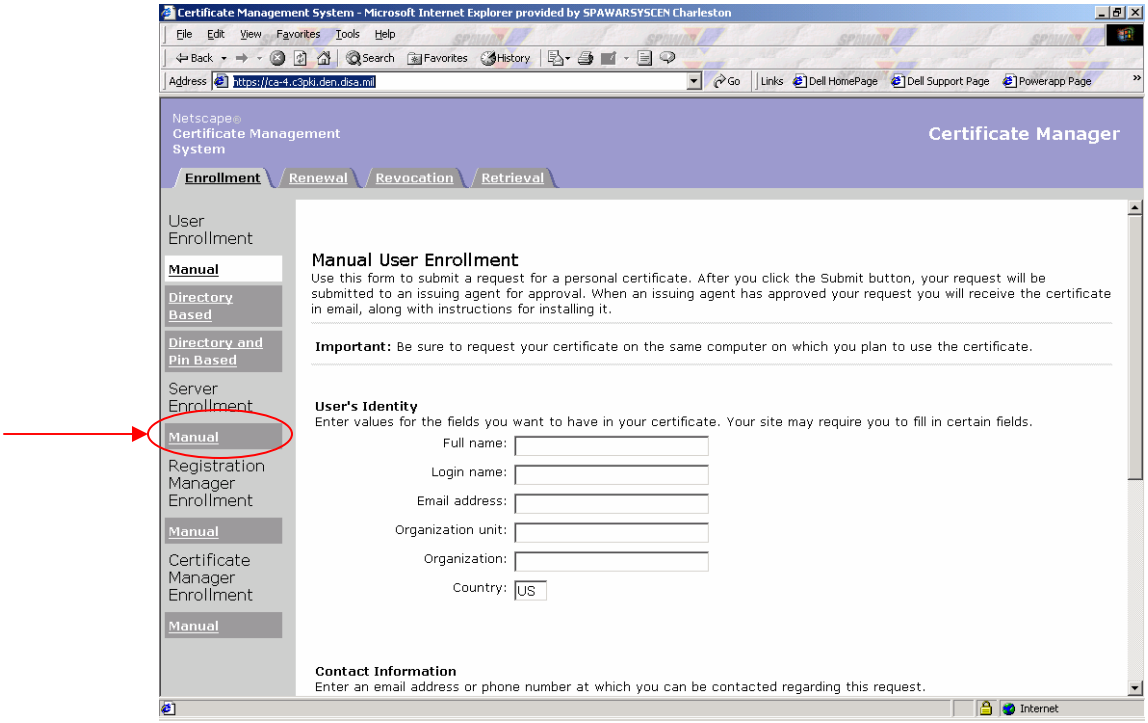
18) **The Completing the Web Server Certificate Wizard Screen** informs you that the certificate request has been successfully completed. This screen displays the file folder and the file name of the certificate request. Click **Finish**.


19) You will now need to open a web browser to communicate with the *Certificate Authority* server to submit your certificate request. You will need to open **Windows Notepad** to copy and paste information from the clipboard during this operation.

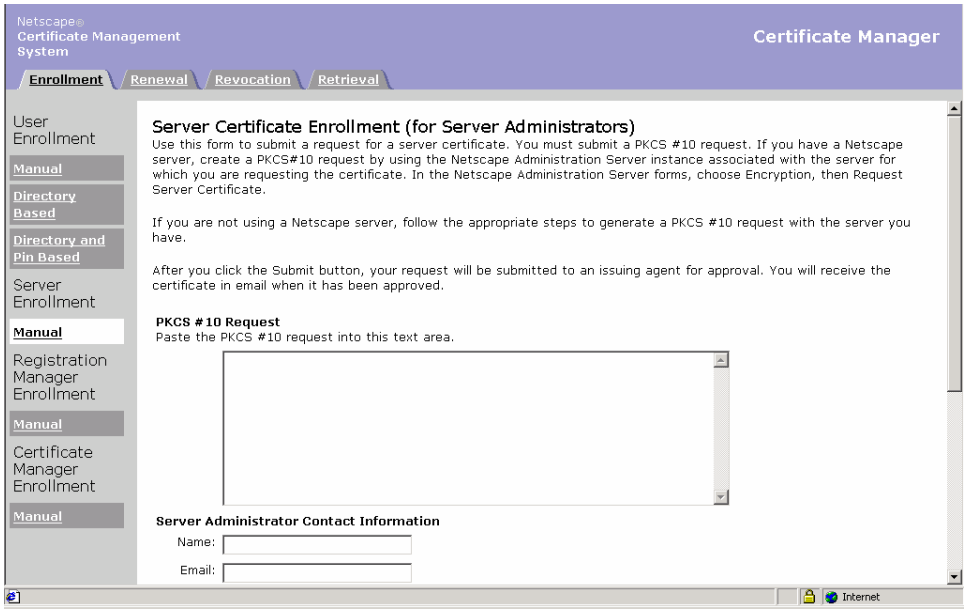
# Requesting a Certificate

After generating a request for a web server certificate, you will submit the request to the **DoD Certificate Authority**. You may use either *Netscape Navigator 4.05* or newer or *Internet Explorer v5.01* or newer.

1) Open your browser and type the URL https://ca-3.c3pki.chamb.disa.mil in the address box. The **Manual User Enrollment** page will display.
2) Click on **Manual** under Server Enrollment.



3) The Server Certificate Enrollment (for Server Administrators) will display.

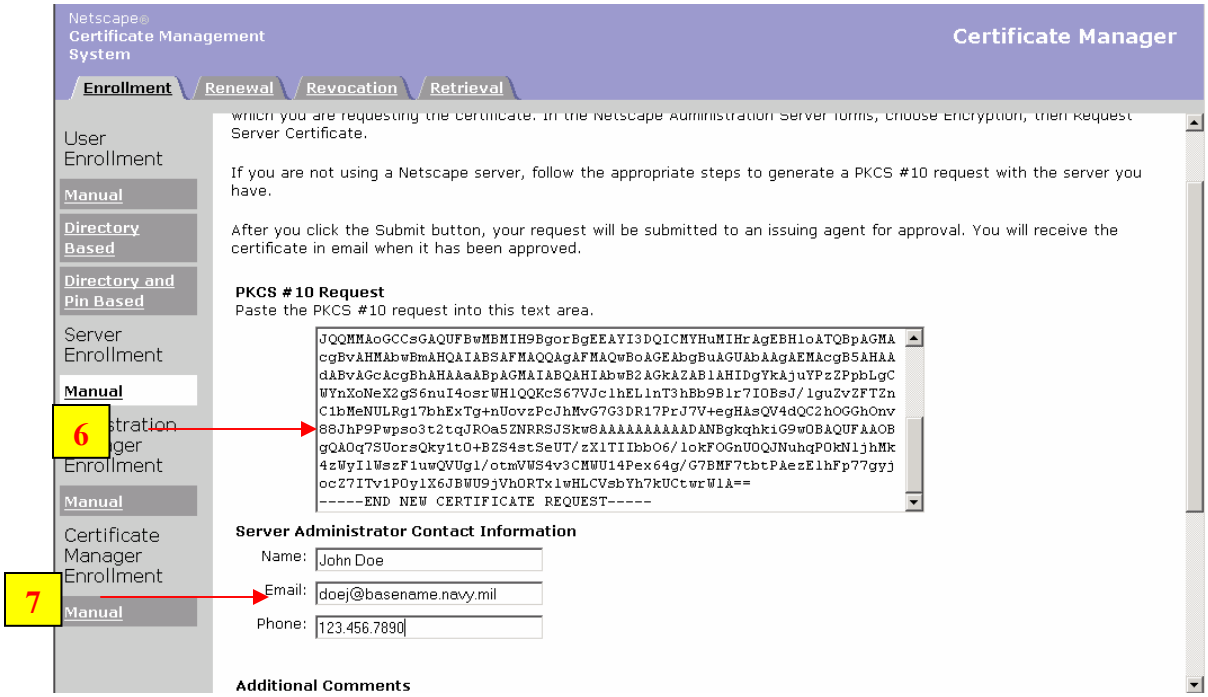



4) Use **Notepad** to open the certificate request (e.g., certreq.txt) file you generated from the web server.

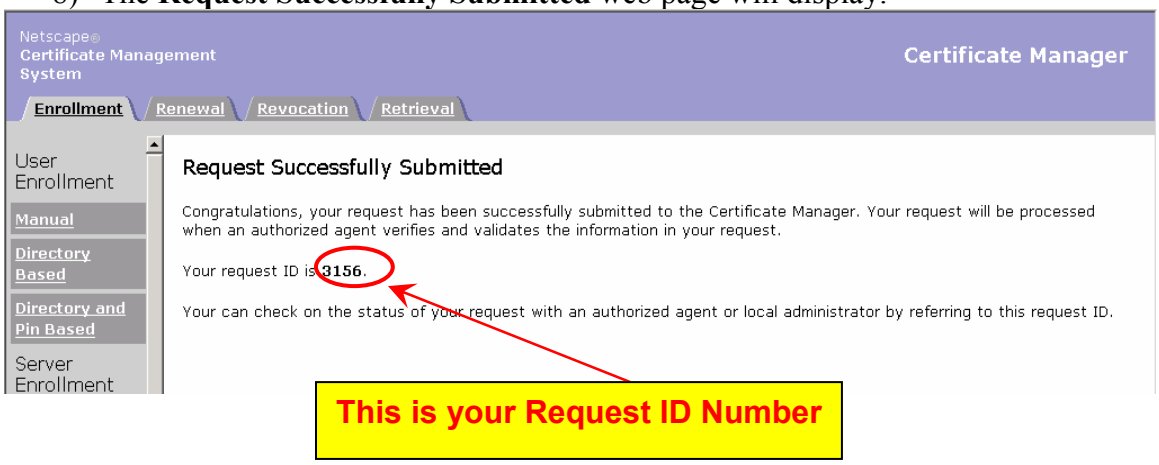
***NOTE:** *Keep the **Server Certificate Enrollment** window displayed in the browser. You will need to copy the certificate information from Notepad file into this browser screen.*

Highlight the text including **BEGIN NEW CERTIFICATE REQUEST** header and **END NEW CERTIFICATE REQUEST** trailer with all dashes. To copy this text to the Windows Clipboard, right-click the selected text, and from the shortcut menu, click **Copy**.

5) Click the browser window to make it the active window. The **Request a Server Certificate** page should still be displayed. Click in the **PKCS #10 Request** text area as shown in the next page.
6) Right-click in the text area, and from the shortcut menu, click **Paste** to copy the certificate request information from the Clipboard into the **Server Certificate Enrollment** form.
7) Complete the additional information on this web page. You may need to scroll to see the bottom of the page. Click **Submit Request** to display the **Request Successfully Submitted** screen.




8) The **Request Successfully Submitted** web page will display.




**Print** this screen for your records or write down your **request ID #**. Close all open windows or applications at this time.

# Approval Notification

Approval Notification.

**a.** The next step in the Server Certificate Request Process involves sending an email to your LRA identifying by the request ID number produced at the end of the last section that the certificate request is ready for review. The email must contain the following **(everything in bold is to be typed as shown** with the rest of the information being replaced with what is appropriate for each individual server):

**Reference Number:** xxxx (with xxxx being the request ID number received from the last section)
**Host Name:** www.sample.navy.mil (this is an example only)
**IP Address:** 102.21.12.12 (the server's ip address)
**Region:** East Coast
**Base:** Base Name
**Network System Administrator (NSA):** Sgt John Doe
**System Owner:** SPAWAR
**Security Level:** SBU (Sensitive But Unclassified)
**Applications on Server:** Development versions of the following:
1) SPAWAR PKI Home Page
2) INFOSEC Home Page

**Certification Justification/Requirements:**

- To enable SSL on the server.

a. The LRA/RA, upon receipt of the email, will review the request. If the request was done correctly and is approved, the LRA/RA will send an email that will contain a *Certificate Serial Number (CSN)*. The CSN must be utilized in order to download the certificate. If the request is not approved, the RA will notify the requestor/LRA why.

**b.** If the requestor does not receive anything from the LRA/RA within 1 week after the email was sent, contact the LRA/RA by phone.

**c.** When the email with the CSN has been received, refer to "Server Certificate Enabling for Microsoft Internet Information Server 5.0 Step 2: Obtaining/Installing PKI Server Certificate.